Good afternoon Madam Chairwoman and members of the Subcommittee. I am Sallie McDonald, the Assistant Commissioner for the GSA, FTS, Office of Information Assurance and Critical Infrastructure Protection. I wish to thank you for the opportunity to offer testimony with regard to the National Infrastructure Protection Center (NIPC).

The Federal Computer Incident Response Center or FedCIRC, is a component of GSA's Federal Technology Service. As designated by the Government Information Security Reform Act, it is the central coordination entity for dealing with computer security related incidents affecting computer systems within the Federal civilian agencies and Departments of the United States Government.

FedCIRC was established as a pilot by NIST in 1996 under the Office of Management and Budget (OMB) policy authority as the primary means for civilian Federal agencies to share information on externally generated security incidents and common vulnerabilities. This was recognized as an important activity given the shared risk environment that results from a rise in interconnected systems across government and with connection to the Internet which increases public access. FedCIRC became operational in 1998 and was transferred to GSA. FedCIRC's role was then and is today, one of assisting agencies and sharing information under the overall security policy framework established by OMB. FedCIRC is not intended to substitute for adequate agency security practices or

compete with the role of law enforcement or national security authorities in addressing more serious types of attacks.

GSA reports at least quarterly to OMB on matters such as the number and nature of security incidents reported by the agencies, whether the incidents are the result of exploits of vulnerabilities for which known repairs are readily available, and whether FedCIRC has any specific recommendations for changes to OMB security policy or the National Institute of Standards and Technology (NIST) security guidance.

By definition, a "computer security incident" encompasses any violation of an established or implied security policy or statute. Incidents include but are not necessarily limited to activities such as attempts to gain unauthorized access to government systems or data, disruption of service, unauthorized use of computing resources and changes to system hardware or software without consent of the owner.

FedCIRC and the NIPC are both crucial to effective cyber defense but serve differing roles to the Federal community. FedCIRC's role is to provide incident response and handling support to agencies. When an agency reports an incident, FedCIRC works with the agency to identify the type of incident, contain any damage to the agency's system, and provide guidance to the agency on recovering from the incident. The NIPC, on the other hand, collects incident reports and is responsible for providing threat assessments, vulnerability studies, warnings, and the coordination of the Federal government's investigative response to attacks.

Upon receiving an incident report from a Federal agency, FedCIRC evaluates and categorizes the incident with respect to its impact and severity. If criminal activity is indicated, FedCIRC informs the reporting agency of the requirement to immediately contact their Inspector General or the NIPC. Should the incident appear to have originated from a foreign country, FedCIRC categorizes it as having potential national security implications and immediately contacts both the NSIRC and the NIPC. The reporting agency is subsequently notified of such action by FedCIRC. There is ongoing discussion between the NIPC and FedCIRC to improve information sharing and analytic efforts and to educate agencies of the value of rapid involvement of the NIPC when incidents occur. When the escalation of an incident has the potential for widespread proliferation or damage, FedCIRC and the NIPC routinely pool their information and skills. FedCIRC is frequently requested by the NIPC to collaborate with multiple sources and the affected agency or agencies to gather more detailed information specific to a given incident. Cyber-incidents involving a pending or potential investigation are jointly handled in a manner that preserves sensitive cyber-evidence without adverse impact to the affected agency's mission functions or violation of constitutional law and applicable privacy statutes.

Effective incident analysis is a product of multiple source data collection efforts, collaboration to quantify related information, and determination of the potential for proliferation and damage. Over the past few years, a virtual network of partners has evolved. This virtual network includes FedCIRC, the NIPC, the National Security

Agency's (NSA) National Security Incident Response Center (NSIRC), the Department of Defense's (DOD) Joint Taskforce for Computer Network Operations (JTF-CNO), industry, academia, and individual incident response components within Federal agencies. Though their missions vary in scope and responsibility, this virtual network enables the Federal government to capitalize on the individual technical strengths, each organization's strategic positioning within the national infrastructure and their access to a variety of information resources. Bridging the disparate boundaries has been a formidable challenge and although there is still work to be done in this area the commitment of the leadership in each organization is on the right path to build the framework for the fluid and cooperative exchange of information. The NIPC, NSIRC, JTF-CNO and FedCIRC are involved in a constant sharing of sensitive cyber-threat and incident data, correlating it with counter-terrorism and intelligence reports to develop strategic defenses, threat predictions and timely alerts. These efforts depend, not on any one participant, but on the unique and valuable contributions of each organization. The NIPC, because of its relationships with industry, is able to solicit additional participation when the government deals with complex analysis issues. This broader spectrum brings together some of the nation's best talent to work on known and developing threats to the cyber infrastructure.

An excellent example of this collaboration is the Government's response to a very recent threat to the cyber infrastructure, know as the "Leaves Worm". This exercise clearly demonstrated how these collaborative relationships work and how each participant's contributions assist in assessing the damage potential. In June, the SANS

Institute, a private sector organization, informed the NIPC of suspicious activities taking place in a large number of systems across the Internet. Widespread scanning was taking place to identify systems previously compromised by a relatively old trojan called "SubSeven." Since SubSeven is for all intents and purposes a remote control program, once identified, the perpetrator could gain full control of the infected system. It was through the SubSeven trojan that the Leaves Worm was being deposited on large numbers of systems around the globe but it was being accomplished without direct intervention by the perpetrator. Clearly we had a new worm of unknown potential and a new delivery method not previously seen. The hacker community, typically vocal in Internet chat rooms about new attacks or malicious code, showed no evidence of any knowledge of the Leaves Worm. The NIPC, DOJ, NSA, FedCIRC, CIA, Department of State, DoD, NCS, NSC, academia, industry software vendors, anti-virus engineers and security professionals quickly activated a collaborative communication network to share details as they analyzed captured code from publicly available web sites that were being used to propagate the worm. It was primarily due to the NIPC's relationship with industry that the volumes of information collected could be rapidly decoded, analyzed and reverse engineered to provide the anti-virus vendors with critical information to develop detection methods for their respective products. This episode serves as an excellent example of the progress various government and private organizations have made in coming together to work toward the common goal of protecting the nation's critical infrastructure.

The NIPC's responsibilities and relationships with various elements in the private sector, its activities as a member of the intelligence community and its lead role for counter-terrorism contribute significantly to the FedCIRC's analytical ability by providing global threat information. Of significant value is the NIPC's ability to reach beyond governmental boundaries and draw on technical skills and information available from components in industry then share those resources with other members of the incident response community. The NIPC staff regularly communicates information to FedCIRC, which in many cases, provides deeper insight into developing situations and often can make the difference between thwarting an attack or tolerating the ensuing damage. Knowing the extent or pattern of incidents as they may impact the private sector, for example, may influence the development of an alert or advisory notice issued to government agencies.

Critical Infrastructure Protection efforts and, more specifically, those for cyber-defense are a relatively new requirement in government and in the private sector. Only recently have these efforts been singled out as a priority for Federal agencies. As government direction for reporting the occurrence of incidents has been promulgated, attempts by agencies to develop related policies and procedures have sometimes been divergent because of differing individual interpretation and misunderstanding. FedCIRC and the NIPC are working diligently to jointly assess problem areas, more clearly define agency responsibilities for reporting incidents, and working with agencies to ensure they have the proper processes and procedures in place to respond to and prevent attacks on their information systems.

The NIPC and FedCIRC routinely exchange information. This exchange is built upon a trust relationship and formalized with the detailing of FedCIRC staff personnel to the NIPC's Watch and Warning Unit. In addition alerts and advisories are frequently generated by the NIPC, NSIRC, or FedCIRC as a collaborative effort and represent a consensus when distributed to our constituents.

As a further example, to simplify the incident reporting process, the NIPC, NSA and FedCIRC have begun efforts to create a single uniform report process that will be used across government. The process will employ common data elements that can be easily shared and integrated into the respective organization's database for shared or unique analysis efforts.

Effective cyber defenses ideally prevent an incident from taking place. Any other approach is simply reactive. FedCIRC, the NIPC, the NSIRC, the Department of Defense and industry components realize that the best response is a preemptive and proactive approach. In order to implement such an approach, all resources must be focused on the common goal of securing the nation's critical infrastructures and the strengths of each organization must be relied upon in order to achieve the most effective results. FedCIRC, the NIPC, DOD, the NSIRC and others comprise a virtual team, each offering significant skills and contributions to the common defense.

**Summary**

Madam Chairwoman, the information presented today highlights the high degree of cooperation among government agencies and the critical and effective relationship that exists between FedCIRC and the NIPC. Though all contribute individually to critical infrastructure protection, our strength in protecting information systems government-wide lies in collaboration and coordination efforts. I trust that you will derive from my remarks an understanding of the cyber-threat and response issues and also an appreciation for the joint commitment to infrastructure protection of FedCIRC and the NIPC. We appreciate your leadership and that of the Committee for helping us achieve our goals and allowing us to share information that we feel is crucial to the defense of our technology resources.